



DOC Code: AP.PRE.REQ

PTO/SB/33 (08-08)

Approved for use through 09/30/2008. OMB 0651-0031

United States Patent & Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it displays a valid OMB control number

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
059643.00747

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed
Name _____

Application Number:

10/748,459

Filed: December 29, 2003

First Named Inventor:

Bing WANG

Art Unit: 2456

Examiner: Kevin S. Mai

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

The review is requested for the reason(s) stated on the attached sheet(s).

Note: No more than five (5) pages may be provided.

I am the

Applicant/Inventor.
 assignee of record of the entire interest.
See 37 CFR 3.71. Statement under
37 CFR 3.73(b) is enclosed (Form PTO/SB/96)

Attorney or agent of record.
Registration No. 58,178

Attorney or agent acting under 37 CFR 1.34.
Registration Number if acting under 37 CFR 1.34 _____


SignaturePeter Flanagan
Typed or printed name1.703.720.7864
Telephone numberMay 4, 2009
Date

NOTE: Signatures of all of the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

*Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Confirmation No.: 7057

Bing WANG

Art Unit: 2456

Application No.: 10/748,459

Examiner: Kevin S. Mai

Filed: December 29, 2003

Attorney Dkt. No.: 059643.00747

For: METHOD AND SYSTEM FOR UNIFIED SESSION CONTROL OF MULTIPLE MANAGEMENT SERVERS ON NETWORK APPLIANCES

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

May 4, 2009

Sir:

Applicant hereby submits this Pre-Appeal Brief Request for Review (“PABRR”) of the final rejections of claims 1-2, 4-9, 11-16, and 18-25 in the above identified application. Claims 1-2 and 4-25 were finally rejected in the Final Office Action dated December 8, 2008 (“Office Action”). Applicant filed a Response to the Office Action on February 9, 2009 (“Applicant’s Response”). The Response cancelled claims 10 and 17. The Office issued an Advisory Action dated April 8, 2009 (“Advisory Action”) indicating the cancellation of claims 10 and 17 had been entered for appellate purposes. Applicant hereby appeals these rejections and submits this PABRR. A Notice of Appeal is timely filed concurrently herewith.

Claim 25 was rejected under 35 U.S.C. §101 because the claimed invention is allegedly directed to non-statutory subject matter. The Examiner alleged that the specification defines “computer-readable medium” in such a way that it “could include signals” and, thus, the claimed subject matter is non-statutory. Applicant respectfully traverses this rejection.

The Office Action has not identified any place where the term “computer-readable medium” is defined in such a way as to include signals. Quite to the contrary, the specification provides at page 5, line 18, and following several examples of computer readable media without ever once identifying a signal as such a medium. A computer readable medium is recognized as patentable subject matter under §101 and U.S. patent practice. Support for the definition of a

computer readable medium is provided by *In re Lowry*, 32 F.3d 1579, 1583-1854, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994), which states: “When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized” (see §2106.01 of the MPEP). Thus, under U.S. precedent and the MPEP, the claims recite statutory subject matter.

Claims 1-2 and 4-25 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2001/0047406 of Araujo *et al.* (“Araujo”). Applicant respectfully traverses this rejection.

Araujo generally relates to an apparatus and accompanying methods for providing, through a centralized server site, an integrated virtual office environment, remotely accessible via a network-connected web browser, with remote network monitoring and management capabilities. In Araujo, a front end (a service enablement platform (SEP)) to one or more office servers on a LAN is connected to both the WAN and LAN and acts as a bridge between the user and the user’s office applications. The front end also acts as a protocol translator to enable bi-directional, web-based, real-time communication to occur between the browser and each such application.

The Office Action has recognized that Araujo does not explicitly disclose that the feature of establishing a session between a unified session manager (SEP 200 of Araujo in the Office Action’s view) and a management server associated with an application comprises authenticating the unified session manager to the management server. However, the Office Action appears to have considered that this is implicit in Araujo, referring to paragraph [0109] of Araujo, which discloses that all information transfer for the Netilla virtual office is protected by SSL.

As such, the Office Action considered that the SEP and the application servers of Araujo communicate using SSL and that using SSL is known to inherently include an authentication step. Accordingly, the Office Action concluded that the SEP and the application servers authenticate themselves utilizing the SSL protocol in Araujo.

The Office Action’s analysis is incorrect. While the Office Action is correct that the SSL protocol can include an authentication step, the Office Action is incorrect that the SEP and the application servers communicate using SSL in Araujo. Although Araujo does state in paragraph

[0109] that for the Netilla virtual office, all information transfer is protected by SSL, if one reads further from this disclosure, it is made clear by Araujo that SSL encryption and decryption is only utilized for all communications to and from the remote client via the WAN and is not in fact used for communications between the SEP and the LAN including the application servers.

In paragraph [0109] of Araujo, it is explained that when an incoming packet is received at the SEP from the client device via the WAN connection, the open SSL module 304 performs SSL processing on the packet. This may implicitly involve authenticating the packet as suggested by the Office Action. It is then stated that after SSL processing, the HTTP request is extracted and sent to the virtual office software 400 for translation into a form suitable for use by a desired office application. Once virtual office software 400 has properly processed the information, by providing suitable protocol conversion, that information flows directly from software 400 to the office application. Thus, it is clear that the incoming packet is authenticated and decrypted prior to extraction of the content of the packet extraction and subsequent translation by the virtual office software 400. The HTTP request is thus extracted, translated and sent directed to the office application without passing back via the open SSL module 340 for encryption prior to being sent to the application server. As such, there is no SSL encryption used for communications between the SEP and the application server.

The aforementioned interpretation (*i.e.* Applicant's interpretation) is confirmed as being correct with further reference to the disclosure in paragraph [0111] of Araujo, which describes the processing of packets received by the SEP from the LAN. These packets are received along data path 402 shown in Figure 3b. This path flows through to the virtual office software 400 without passing through web server 350 and without calling on the open SSL module 340. The virtual office software 400 generates an appropriate HTML page and only then passes the HTML page to web server 350. The web server 350 then calls on the services of the open SSL module 340 to encrypt the HTML page and send it to the remote client via the WAN.

In light of the above, it is clear that the mention of "all information transfer is protected by SSL" in paragraph [0109] of Araujo actually relates to all information transferred between the remote client and the SEP via the WAN. No authentication and encryption protocols are utilized between the SEP and the LAN.

If there is any further doubt regarding the aforementioned analysis, Applicant respectfully further points out that the reason no encryption protocol is required in Araujo between the SEP and the LAN is that the SEP is authenticated during an initial installation process with the centralized administrative website (referred to as “customer care centre” (CCC)). This is described, for example, in paragraphs [0038] to [0041] of Araujo.

In light of the above, it is clear that there is no disclosure or suggestion in Araujo that establishing a session between the SEP and management server associated with an application comprises authenticating the SEP with the management server associated with the application. Rather, the SEP in Araujo is authenticated with a centralized administrative website (CCC) during installation and subsequent communications between a remote client and the SEP via the WAN are encrypted and decrypted using SSL.

The arrangement described in Araujo is adapted for use in small to medium sized organizations and specifically for remotely accessing an internal office network remotely by employees. A centralized administrative website (CCC) is used for remote network monitoring and management functionality. No authentication or encryption protocols are required between the SEP and the LAN as these are all located within the local office network environment. In contrast, certain embodiments of the present invention are directed to a method and system for managing multiple management servers via a single unified session manager to provide a unified session control for general services over the internet to internet users who may not necessarily be employees looking to remotely access a local office network. As such, the applications and management servers associated therewith may not be provided in a safe office intranet environment. Accordingly, the arrangement of Araujo is not appropriate for the use intended for the present invention. For more general internet usage, it has been found by the present inventors to be advantageous that when a request is received from a client device for accessing an application, the step of establishing a session between a unified session manager and a management server associated with the application comprises authenticating the unified session manager to the management server. Such an authentication process is not required in Araujo.

Accordingly, it has been demonstrated that Araujo fails to disclose or suggest at least “wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually

transparent to the client device" (as recited in claim 1), or the similar recitations found in independent claims 8, 15, 19, and 23-25, each of which has its own respective scope. It is, therefore, respectfully requested that the rejection of claims 1, 8, 15, 19, and 23-25 be withdrawn.

It is noted that the Advisory Action argued that, despite the distinctions above, "this alone is not enough to determine that SSL would not be used between the SEP and the LAN." Applicants respectfully note, however, that the burden is on the Office Action to positively demonstrate disclosure of the feature in the cited art, not on Applicants' to prove non-disclosure. Accordingly, the appropriate standard is whether the disclosure is sufficient to positively establish disclosure of the claimed features. In this instance, it should be apparent that the disclosure in the art is not sufficient, as the art does not disclose the subject matter either explicitly, implicitly, or inherently.

Accordingly, the Office Action's rejections of claims 1-2, 4-9, 11-16, and 18-25 are in clear error for at least the reasons discussed above. Reconsideration and withdrawal of the rejections, in view of the clear errors in the Office Action, is respectfully requested. In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,


Peter Flanagan
Attorney for Applicant
Registration No. 58,178

Customer No. 32294

SQUIRE, SANDERS & DEMPSEY LLP
8000 Towers Crescent Drive, 14th Floor
Vienna, Virginia 22182-6212
Telephone: 703-720-7800, Fax: 703-720-7802

Enclosures: Notice of Appeal, Petition for Extension of Time, PTO/SB/33 Form,
Check No. 20825.